United States v. Shacar
21-cr-30028-MGM
EXHIBIT “13”

O caso envolve um grupo de investigações e processos relativos à exploração sexual de crianças na *Deep Web.* Na investigação, conduzida pelo Ministério Público Federal e aproximadamente doze forças policiais de todo o mundo (Estados Unidos, Reino Unido, Austrália, Canadá, Nova Zelândia, Alemanha, Portugal, Itália, Noruega, França e Áustria), foi possível verificar a atuação de grande grupo criminoso transnacional, voltado para o cometimento sobretudo de crimes de venda, disseminação, produção e armazenamento de pornografia infantil (arts. 240, 241, 241-A e 241-B do ECA) e de estupro, inclusive de vulnerável (arts. 213 e 217-A do Código Penal), ocorridos pelo menos desde 2013 em *hidden services* da *Deep Web.*

O objetivo principal da *Deep Web* é proteger a identidade dos usuários por meio da circulação dos dados através de uma rede distribuída de computadores, chamados nódulos. Isso resulta no encobrimento do *IP* (*internet protocol*), essencial para a identificação dos criminosos cibernéticos nas investigações mais comuns. Além de encobrir os endereços *IPs* de usuários individuais, a rede TOR também permite ocultar a localização física de vários serviços da *internet*, formando os chamados "serviços ocultos" (*hidden services*). Tais características aumentam sobremaneira a dificuldade da persecução criminal.

No caso, os referidos serviços ocultos eram conhecidos pelos sugestivos nomes de *Baby Heart*, *Boy Vids* 4.0, *HurtMeh*, Anjos Proibidos BR e *Loli Lust*. Somados, os usuários desses fóruns chegavam a 1.839.831 membros, de diversas nacionalidades e línguas do mundo, como alemão, chinês, árabe, húngaro, entre outros, os quais compartilhavam e publicavam conteúdo de abuso sexual infantojuvenil, desde fotos e vídeos a manuais de estupro. As plataformas tinham as seguintes características principais:

a) *Baby Heart* ("coração de bebê", em tradução livre): destinado ao material de abuso sexual de bebês e crianças de 0 a 5 anos de idade;

b) *HurtMeh* ("machuque-me", em tradução livre): destinado ao compartilhamento de imagens e vídeos de abuso sexual de crianças com ênfase em material *hurtcore* (abuso sexual com violência), incluindo sadismo, tortura e morte de crianças;

c) Anjos Prohibidos: dedicado ao compartilhamento de material de abuso sexual de meninos e voltado exclusivamente aos falantes de português;

d) *BoysVids4.0*: destinado ao compartilhamento de abuso sexual de meninos; e,

e) *Lolilust* (algo como "desejo por lolitas", em tradução livre, com alusão ao livro "Lolita", do escritor russo Vladimir Nabokov): destinado ao compartilhamento de imagens de abuso sexual de meninas.

A prisão, em 2017, em Portugal, de um dos administradores do mencionado *Baby Heart*, levou a uma investigação na qual surgiram provas que levaram à prisão e denúncia, em Recife/PE, de outro seu administrador.

Na fase final do processo, o Ministério Público Federal foi procurado para acordo de colaboração premiada com esse administrador local, o qual informou ter relação direta, pela *Deep Web*, com o possível mantenedor de vários serviços ocultos de pornografia infantil, um dos alvos mais procurados do mundo pelos órgãos de repressão penal. O MPF confirmou, por meio de contatos com o *Federal Bureau of Investigation* (FBI), a existência e importância dessa pessoa. Segundo o FBI, ele mantinha aproximadamente 70% do conteúdo de pornografia infantil de toda a *Deep Web* no mundo. Então, o MPF celebrou a colaboração.

Homologada a colaboração premiada, obteve-se, em feito incidental, autorização para infiltração policial na *internet*, com os agentes policiais, o Ministério Público Federal e o colaborador. O papel do colaborador foi passar informações relevantes sobre termos comuns entre criminosos dos serviços ocultos e travar contatos diretos com o mantenedor dos serviços criminosos a fim de obter dados para sua identificação.

O estreitamento do contato com o mantenedor dos serviços na infiltração e o auxílio técnico, autorizado judicialmente, com o FBI, levaram à identificação do endereço *IP* do alvo.

A partir do IP, requisitaram-se os dados cadastrais na provedora do serviço de *internet*. O respectivo assinante era um analista de sistemas que trabalhara com provedores de serviços de aplicação e de hospedagem na *internet*, perfil compatível com o investigado.

O principal suspeito, certamente tinha muito conhecimento de informática, pois conseguia manter serviços de pornografia infantil desde 2013, o que trazia dificuldades adicionais à investigação. Realmente, nesse cenário, muito possivelmente todos os

equipamentos eram criptografados, acessíveis mediante senhas de grande complexidade e deletáveis com facilidade mesmo à distância. Portanto, era necessário obter acesso a eles ainda em funcionamento e capturar as senhas de administrador de modo a possibilitar a perícia e identificar os usuários inscritos. Como muitos dos usuários afirmavam e mesmo postavam imagens inéditas de abuso, a descoberta de sua identidade poderia levar ao resgate de crianças e adolescentes vitimadas.

Novamente com autorização judicial, foi efetivado o afastamento do sigilo e a interceptação do fluxo das comunicações em sistemas de informática e telemática dos pontos de acesso à *internet* da residência do mantenedor dos *hidden services*.

Na interceptação telemática, monitorou-se, com apoio da NCA inglesa, todo o fluxo de dados do investigado, em meio investigativo inédito no Brasil. Concluiu-se que, do total de 445 GB analisados, aproximadamente 374,108 GB (85,53%) correspondiam a tráfego TOR e que a elevada média diária de dados indicava que o computador alvo da interceptação atuava como servidor ou *relay* (roteando tráfego de terceiros), não como mero cliente ou usuário.

Ante tais provas novas, o Ministério Público Federal obteve autorização para: a) ação controlada; b) interceptação telefônica em terminais do investigado ou de pessoas ligadas a ele; c) obtenção de conteúdo armazenado em provedor de *e-mail* e de aplicações de *internet*; d) captação ambiental em residência, de modo a possibilitar a gravação das senhas quando digitadas por ele; e, e) busca e apreensão, inclusive exploratória, em seu domicílio.

O segundo período de interceptação telemática foi marcado pelo uso de uma técnica de deanonimização (retirada do anonimato, ínsito à *Deep Web*) auxiliada pelo FBI. Essa força policial gerou sinais para simular acesso em grande volume aos *hidden services* possivelmente mantidos pelo principal investigado. Dessa forma, interceptada a conexão do endereço, foi possível distinguir entre os períodos de tráfego normal recebido pelo *hidden service* e os períodos em que o sinal foi enviado pela aplicação. Ao aumento do volume de acessos, simulado pelo sinal gerado, correspondeu o aumento do volume de dados interceptados. Assim, a técnica corroborou a manutenção dos serviços na residência.

Também houve a interceptação telefônica de números vinculados a esse investigado, o que se revelou útil porque se captaram diálogos entre ele e a provedora de *internet* dando

conta de que o serviço não estava funcionando. Nesse período, os *hidden services* permaneceram fora do ar, de forma que a autoria delitiva foi reforçada.

A busca exploratória, técnica inédita que consistia em autorização para entrar na residência do alvo, na sua ausência, a fim de analisar a possibilidade de instalar câmeras de captação ambiental (ideia posteriormente descartada), de utilizar dispositivo de captura de dados digitados ou transmitidos pelo *mouse* (*keylogger* e *mouselogger*) e de copiar dados de equipamentos eletrônicos, também trouxe resultados dignos de nota.

No dia 8/3/2019, acessou-se o painel de disjuntores do condomínio em que o mantenedor residia. Assim, desligou-se a energia elétrica do imóvel, acarretando a saída do ar dos *hidden services*, que estavam *online* logo antes do desligamento. No dia 12/3/2019, nova busca exploratória constatou diversos computadores, HDs externos e internos, *pen drives* e outras mídias, decidindo-se copiar futuramente o máximo possível de dados.

No dia 5/6/2019, foi realizada a segunda entrada exploratória na residência, em que foram instalados *keyloggers* no interior de dois teclados. Com essa técnica, de expertise repassada pela polícia inglesa, todos os dados digitados pelo investigado seriam captados e armazenados. Entre esses dados, os principais eram as senhas de administrador dos fóruns. Também se aproveitou a ocasião para uma cópia completa do disco rígido do servidor, ocasionalmente desprotegido, para futuro exame pericial, em caso de posterior destruição do equipamento ou de ineficácia dos *keyloggers*.

Após a instalação dos *keyloggers* no interior dos dois teclados, forçou-se novamente o desligamento de energia de todos os servidores, para que o investigado precisasse reiniciá-los e inserir a sua senha, agora captável. A estratégia funcionou.

No dia seguinte, 6/6/2019, foram cumpridos o mandado de prisão preventiva e os mandados de busca e apreensão, possibilitando apreender diversas mídias de armazenamento na residência do investigado, algumas inclusive em funcionamento.

Tais mídias foram copiadas e periciadas, para subsidiar a continuidade das investigações de abusadores de crianças no Brasil e no mundo, já que havia autorização judicial de compartilhamento do material.

Nesse material, havia 2.042.408 arquivos de cenas de sexo explícito ou pornográficas de crianças ou adolescentes. Encontraram-se também arquivos referentes aos mencionados *hidden services*, somente acessíveis em razão da captura das senhas pelos *keyloggers*.

Outros meios de prova, como o afastamento do sigilo de *e-mail*, do sigilo bancário, do sigilo fiscal, da ERB de seu celular e de dados do seu uso do aplicativo Uber, além do acompanhamento físico do investigado quando fora de sua residência, mostraram-se úteis na instrumentalização da busca exploratória e na corroboração e descoberta de crimes.

Já o compartilhamento com outros países levou, por exemplo, à libertação de um menino, preso e abusado há quase dois meses, na Rússia e a diversas investigações e processos no Brasil e em outros lugares do mundo.

Ademais, a NCA produziu relatórios com os *logs* de conexão e *IPs* de 68 usuários dos fóruns no Brasil, autores de crimes tais como estupro de vulnerável e produção, divulgação e aquisição de fotografias e vídeos contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Há, entre eles, agentes delitivos processados por crimes da mesma espécie. Também se destacam as provas relativas a possível mantenedor de novos fóruns de pornografia infantil.

O aprofundamento da investigação em relação a esses 68 novos agentes delitivos, em inquérito mantido na 36ª Vara Federal de Pernambuco por conexão, levou a uma nova fase da operação, com quebras de sigilo, 8 prisões preventivas e 105 mandados de busca e apreensão.

A execução dessa nova fase, em 3/12/2021, trouxe o cumprimento de todos os 8 mandados de prisão preventiva e 23 prisões em flagrante por crimes do art. 241-B do ECA. Análises preliminares nos equipamentos apreendidos levaram a novos crimes aos menos dos arts. 240 do ECA e 217-A do Código Penal. E o que é mais, permitiu o resgate de 3 crianças vítimas de possível abuso sexual. As provas subsidiarão novas investigações e processos em juízos diversos.

Por fim, ressalto que houve autorização judicial para a "divulgação a respeito da existência da operação, do processo e dos fatos a ele relacionados, desde que a partir deles não seja possível identificar as vítimas e os investigados."